



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: 267-930-4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 13, 2018

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Pharmacy Times Office of Continuing Professional Education, LLC (“PTCE”), 2 Clarke Drive, Suite 100, Cranbury, NJ 08512, and are writing to notify your office of an incident that may affect the security of information relating to seven hundred ninety-seven (797) Washington residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PTCE does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. Through this ongoing investigation, PTCE determined on September 17, 2018 that a file containing PTCE data had been publicly available between May 11, 2018 and July 6, 2018, and may have been subject to unauthorized access by an unknown party on or about July 6, 2018. On or around October 12, 2018, PTCE confirmed the file contained information including personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

PTCE began providing notice to the individuals potentially affected by this incident as soon as their address information was confirmed. The personal information impacted by this event may include the following: name and Social Security number. Out of an abundance of caution, PTCE also provided notice of this incident to individuals who did not have statutorily protected personal information impacted. To date, PTCE has not received any reports of the misuse of this information.

Notice to Washington Residents

On November 13, 2018, PTCE began providing written notice of this incident to affected individuals, which includes seven hundred ninety-seven (797) Washington residents. This includes seven hundred three (703) individuals whose personal information under state law may have been accessible. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

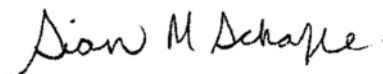
Upon discovering the potential unauthorized access to the data file, PTCE moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. PTCE is also working to implement additional safeguards to protect the security of information in its system.

PTCE is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to one (1) year of credit and identity monitoring services, including identity restoration services through Kroll, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, PTCE is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. PTCE is also providing written notice of this incident to other state regulators and the major consumer reporting agencies, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4799.

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS:emp
Enclosure
cc: Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
Email: securitybreach@atg.wa.gov

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Pharmacy Times Office of Continuing Professional Education, LLC (“PTCE”) is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

What Information Was Involved? The review of the file determined that the following types of your personal information was publicly accessible: <<ClientDef1(INSERT FIRST VARIABLE ELEMENTS)>>. To date, PTCE has not received any reports of the misuse of your information.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Jim Palatine, RPh, MBA
President



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until **February 1, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
[www.experian.com/fraud/
center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
[www.transunion.com/fraud-victim-
resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 804 Rhode Island residents impacted by this incident.



<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Pharmacy Times Office of Continuing Professional Education, LLC (“PTCE”) is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

What Information Was Involved? The review of the file determined that the following types of your personal information was publicly accessible: <<ClientDef1(INSERT FIRST VARIABLE ELEMENTS)>>. In addition to the forgoing, the following additional information may have also been publicly accessible: <<ClientDef2(INSERT SECOND VARIABLE ELEMENTS)>>. While this second set of information may not be considered protected data under applicable statutes, you are nonetheless being provided with notice out of an abundance of caution. To date, PTCE has not received any reports of the misuse of your information.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, we are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Jim Palatine, RPh, MBA
President



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until **February 1, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
[www.experian.com/fraud/
center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
[www.transunion.com/fraud-victim-
resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 804 Rhode Island residents impacted by this incident.